CLAIMS

1. (previously presented) A portable device comprising:

a microprocessor;

a non-volatile memory coupled to the microprocessor; and

a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise.

2. (previously presented) The portable device as recited in Claim 1 wherein the biometrics-based authentication module is a fingerprint authentication module.

3. (previously presented) The portable device as recited in Claim 1 further comprising a universal serial bus (USB) connector for coupling with another USB-compliant device.

4. (previously presented) The portable device as recited in Claim 1 wherein the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the portable device.

5. (previously presented) The portable device as recited in Claim 1 wherein the non-volatile memory comprises flash memory.

6. (previously presented) The portable device as recited in Claim 1 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.

7. (currently amended) A portable device comprising:

a bus;

a microprocessor coupled to the bus;

a non-volatile memory coupled to the bus; and

a biometrics-based authentication module coupled to the bus, wherein under the control of the microprocessor the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (2) store the first biometrics marker in the non-volatile memory; (3) capture a second biometrics marker; and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker; and wherein the microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module.

8. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is a fingerprint authentication module.

9. (previously presented) The portable device as recited in Claim 7 further comprising a universal serial bus (USB) device controller coupled to the bus and a USB connector coupled to the bus, such that the portable device is capable of communicating with a host platform via the USB connector.

10. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is structurally integrated with the portable device in a unitary construction and comprises a biometrics sensor being disposed on one surface of the portable device.

11. (previously presented) The portable device as recited in Claim 7 wherein the non-volatile memory comprises flash memory.

12. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory.

13. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to direct the biometrics-based authentication module to capture and store the first biometrics marker provided that no biometrics marker has been stored in the non-volatile memory.

14. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to enable access to the non-volatile memory upon a determination of authentication success by the biometrics-based authentication module.

15. (canceled)

16. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.

17. (currently amended) A biometrics-based authentication method implemented using a portable device, the method comprising the steps of:

(a) obtaining a first biometrics marker from a user with a biometrics sensor installed on the portable device;

(b) retrieving a registered biometrics marker from a non-volatile memory of the portable device, the registered biometrics marker having been stored therein during a registration process;

(c) comparing the first biometrics marker against the registered biometrics marker;~~and~~

(d) denying the user access to the non-volatile memory provided that a match is not identified in said step (c); and

~~(d)~~(e) signaling an authentication success provided that a match is identified in said step (c).

18. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein the registered biometrics marker is a fingerprint.

19. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein the registered biometrics marker is stored in an encrypted format.

20. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein said step (d) comprises granting the user access to the non-volatile memory.

21. (canceled)

22. (previously presented) The biometrics-based authentication method as recited in Claim 17 further comprising the step of providing the user with a bypass authentication procedure provided that a match is not identified in said step (c).

23. (new) A unitary portable data storage device having biometrics capability which can be directly plugged into a universal serial bus (USB) socket of a host computer, the device comprising:

a housing;

a fingerprint module, at least a portion of which is housed within the housing, the fingerprint module including a sensor disposed on an exterior surface of the housing;

a memory including non-volatile memory, the memory housed within the housing and coupled to the fingerprint module and is configured to store at least one fingerprint template as well as user data;

a memory controller housed within the housing and coupled to the memory, the memory controller controlling access to the memory;

a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer; and

a USB device controller housed within the housing, the USB device controller enabling the unitary portable data storage device to communicate with the host computer via the USB protocol;

wherein the fingerprint module is configured to (1) receive a fingerprint sample from a user placing a finger on the sensor; (2) compare the fingerprint sample with said at least one fingerprint template; and (3) reject a request from the user to access the user data stored in the memory provided that the comparison in said step (2) results in no match.

24. (new) The unitary portable data storage device as recited in Claim 23 wherein at least a portion of the USB plug protrudes from the housing to facilitate direct coupling of the unitary portable data storage device to the USB socket of a computer.